Secure Messaging PP

Version 0.21

November 9, 2000

Prepared By: NSA, BA&H, & TASC
Prepared For: NSA

Foreword

This Secure Messaging Protection Profile has been written to provide a basis for designing a Simple Message Transfer Protocol (SMTP) messaging application in accordance with the requirements of S/MIME version 3. The Protection Profile is in no way designed to replace mandatory security requirements or lessen the security posture of already developed applications. Instead, its intention is to be used as a guide to develop products to meet the Objectives, Functional Security and Assurance Requirements to counter the identified Threats, while remaining within the Evaluation Assurance Level 3 of the Common Criteria. Comments concerning this Protection Profile may be sent to National Security Agency, V32, 9800 Savage Road, Fort George G. Meade, Maryland 20755.

Table Of Contents

List of Tables:

1 Introduction

1.1 Identification

Title: Secure Messaging Protection Profile

Authors: National Security Agency (NSA), Booz-Allen &Hamilton, Inc. (BAH), & The Analytical Sciences Corporation (TASC)

Vetting Status:

CC Version: 2.1 Final

General Status:

Registration:

Keywords: Secure Messaging Transport Protocol, SMTP, S/MIME, PKI, mail

1.2 Protection Profile Overview

1.2.1 Background

Secure Multi-purpose Internet Mail Extension (S/MIME) standards are being adopted to provide a secure messaging application.

1.2.2 Purpose

The SMPP identifies the requirements necessary to develop a distributed, multi-user secure messaging application system

SMPP accomplishes its purpose by:

- Describing a scalable secure messaging application by identifying its use and security requirements
- Specifying the environment for which the secure messaging application is intended
- Providing specific instructions in the form of refinement statements of its Objectives and Functional Security Requirements.

1.2.3 Scope

Type of system. SMPP defines a distributed, multi-user secure messaging application system.

Type of access. Is a combination of role-based and mandatory access control. There are two roles required, the Messaging Administrator and User. Message labels are enforced.

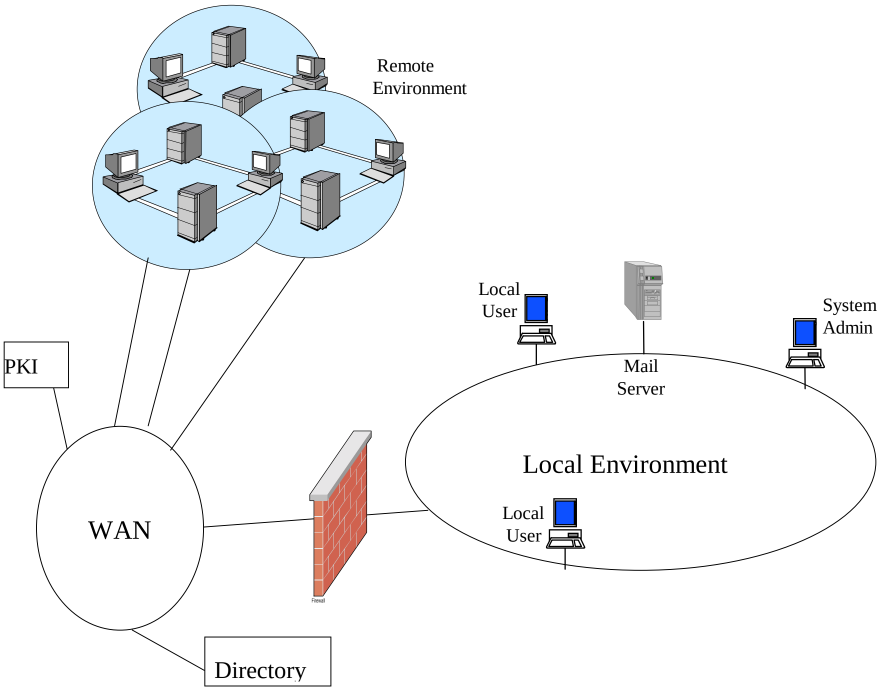
Nature of use. The application will be used within a protected enclave to create, distribute, and receive signed, encrypted, or plaintext messages.

2 TOE Description

The purpose of this Target of Evaluation (TOE) is to provide secure business-grade electronic mail services within and among information technology environments. The TOE will interface with other systems to include: directories for addressing, Public Key Infrastructure (PKI) for certificates, and other E-mail systems for communications, as depicted in figure 1.

Specifically, the TOE is a secure PK-enabled SMTP/MIME messaging application that is compliant with S/MIME version 3. The TOE includes all client and server messaging functions. The TOE does not include operating system or communication applications and services. The TOE will be scaleable for a distributed global network. The TOE will provide a labeled message environment. Security of messages will include the confidentiality and integrity of message body and envelope, the non-repudiation of originator and recipient of messages, and accountability and authenticity of all TOE users.

Users of the TOE will include end users and messaging administrators. Both users will be required to use strong authentication to access TOE resources and perform their assigned functions of the messaging application (e.g., client or server related) according to their specific roles.



3 TOE Security Environment

The TOE environment is both a physically and a logically secure environment that can operate in a mode capable of protecting the transmitted or stored information at the highest classification level of messages in this environment. Additionally, the messaging application will coexist with other network devices not covered by this protection profile (e.g., Guard systems), to provide for data transmission to lower classification systems. Physical, personnel, and administrative non-technical security is provided by a local support environment and procedures that protect all clients and servers by limiting access to the messaging application and messages to authorized users.

The TOE environment shall implement the Information Assurance (IA) Defense In Depth strategy.

- The TOE environment shall provide appropriate degrees of protection to all computing resources in a multitasking environment. Other applications that may be present include virus detection, malicious code detection, and host-based intrusion detection.

- The TOE environment shall ensure network services provide appropriate confidentiality and defenses against denial of service attacks.

- The TOE environment shall defend the perimeter of information environments (e.g., firewalls, intrusion detection, and uniform policy on protocols allowed across perimeter boundaries).

- The TOE environment shall encompass a cryptographic system, which includes the Certification Authority, certificate revocation processes, Directory Services, Cryptographic Token, and S/MIME agents.

- The TOE environment shall make appropriate use of supporting IA infrastructures (e.g., key management, public key certificates, and directories).

3.1 Secure Usage Assumptions

A.Authenticators_User
The user will not disclose authentication mechanisms (e.g. PIN, password).

A.Authorized_Use
Information shall be used only for its authorized purpose(s).

A.Labels
The user will correctly identify sensitivity labels (e.g. U, C, S, TS) from the set of authorized labels.

A.Message_Secure
The user will select the proper security protections for messages (e.g. sign, encrypt, plaintext).

A.Non_Secure
The TOE will be capable of transmitting and receiving messages to non-secure SMTP mail systems.

A.Resources
Messaging application has no direct interface to operating system resources (i.e., messaging application can not by-pass O/S).

A.Role_Permissions
Individual Certificates working in conjunction with the operating system will determine role permissions to separate the two defined roles: users and messaging administrators.

A.Services
Messaging application has an interface to host operating system and its services, including: storage services, printing services, human-computer interface services (e.g. displays, keyboard, mouse), process controls, time and date services, cryptographic system, and network communications.

A.Transfer_Agent
The messaging application server uses a Message Transfer Agent to communicate with S/MIME agents, PKI services, and a user agent.

A.User_Abilities
The messaging application provides the user-computer graphical interface to compose, read, store, retrieve, delete messages, etc.; and messaging administrator interface to manage global address lists, user access controls, audit files, application configuration, application log files, etc.

A.User_Agent
The messaging application client uses a user agent to communicate with the messaging application server, PKI services, and S/MIME agents.

3.2 Threats to Security

T.Admin_Err_Commit: Administrative errors of commission
A messaging administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application.

T.Admin_Err_Omit: Administrative errors of omission
The messaging administrator fails to perform some function essential to security.

T.Admin_Hostile_Modify: Hostile administrator modification of user or system data
A messaging administrator maliciously obstructs organizational security objectives or modifies the system's configuration to allow security violations to occur.

T.Admin_UserPriv: Administrator violates user privacy policy
Messaging administrator may have full operating system access privileges, which would allow for the disclosure of privacy-related information, which is sensitive information associated with the identity of a user. Prevention of messaging administrator abuses by an application is not possible. Messaging administrator may be constrained by role within the messaging application process space.

T.Component_Failure: A critical system component fails
Failure of one or more system components results in the loss of system-critical functionality.

T.Dev_Flawed_Code: Software containing security-related flaws
A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

T.Failure_DS_Comp: Failure of a distributed system component
Failure of a component that is part of a distributed system will cause other parts of the distributed system to malfunction or provide unreliable results.

T.Hack_AC: Hacker undetected system access
A hacker gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

T.Hack_Comm_Eavesdrop: Hacker eavesdrops on user data communications
Hacker obtains user data by eavesdropping on communications lines.

T.Hack_Masq: Hacker masquerading as a legitimate user or as a system process
A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process.

T.Hack_Msg_Data: Message content modification
A hacker modifies information intercepted from a communication link between two unsuspecting entities before passing it on, thereby deceiving the intended recipient.

T.Hack_Social_Engineer: Social engineering
A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

T.Malicious_Code: Malicious code exploitation
An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of system assets.

T.Power_Disrupt: Unexpected disruption of system or component power
A human or environmental agent disrupts power causing the system to lose information or security protection.

T.Repudiate_Receive: Recipient denies receiving information
The recipient of a message denies receiving the message, to avoid accountability for receiving the message or to avoid obligations incurred as a result of receiving the message.

T.Repudiate_Send: Sender denies sending information
The sender of a message denies sending the message to avoid accountability for sending the message or to avoid obligations incurred as a result of sending the message.

T.User_Abuse_Conf: Hostile user acts cause confidentiality breaches
A user collects sensitive or proprietary information and removes it from the system.

T.User_Err_Conf: User errors cause confidentiality breaches
A user commits errors that cause information to be delivered to the wrong place or wrong person.

T.User_Err_Inaccess: User error makes data inaccessible
A user accidentally deletes user data or changes system data rendering user data inaccessible.

T.User_Err_Slf_Protect: User errors undermine the system's security features
A user commits errors that cause the system or one of its applications to undermine the system's security features.

T.User_Misuse_Avl_Resc: User's misuse causes denial of service
A user's unauthorized use of resources causes an undue burden on an affected resource.

T.User_Modify: User abuses authorization to modify data
A user abuses granted authorizations to improperly change or destroy sensitive or security-critical data.

T.User_Send: User abuses authorization to send data
A user abuses granted authorizations to improperly send sensitive or security-critical data.

3.3 Organizational Security Policies

P.Accountability: Individual accountability
Individuals shall be held accountable for their actions.

P.Availability: Information availability
Information shall be available to satisfy mission requirements.

P.Information_AC: Information access control
Information shall be accessed only by authorized individuals and processes.

P.Integrity: Information content integrity
Information shall retain its content integrity.

P.Lifecycle: System lifecycle phases integrate security
Information systems security shall be an integral part of system lifecycle phases of design, development and integration. Installation, restoration, update, and removal phases can integrate security procedures and options only to the extent provided by the messaging application design

P.Marking: Information marking
Information shall be appropriately marked and labeled.

4 Security Objectives

4.1 Security Objectives for the TOE

O.AC_Admin_Limit: Limitation of administrative access control
Design administrative functions in such a way that the messaging administrators do not automatically have access to user objects (i.e., user accounts), except for necessary exceptions.

O.Active_Content: Limit active content capability
Selection by the client application to active/deactivate active content execution in order to deter embedded malicious code.

O.Adm_Limits_Bindings: Limit an administrator's ability to modify user-subject bindings

Limit the messaging administrator from modification of user-subject bindings in an effort to deter messaging administrators and users from acting without accountability.

O.Adm_User_Att_Mod: Limit messaging application administrator's modification of user attributes
Deter the messaging administrator from maliciously modifying users' attributes. Such modifications could allow unauthorized user actions or denial of service to a legitimate user.

O.Admin_Guidance: Administrator guidance documentation
Deter administrator errors by providing adequate messaging administrator guidance.

O.Apply_Code_Fixes: Apply patches to fix the code
Apply patches to fix the code when vulnerabilities in the code are discovered.

O.Atomic_Functions: Complete security functions or recover to previous state
Recover automatically to a consistent, secure state if a security function does not complete successfully in the presence of certain types of failures (e.g., certificate validation failures, revoked certificate detection.)

O.Audit: Auditing capabilities
Provide information about past user behavior to an authorized user through system mechanisms to discover system misuse and provide a potential deterrent by warning the user. Auditable actions shall be defined by selection of individual roles. The audit record shall contain date/time of the action, location of the action, and the entity responsible for the action.

O.Crypto_AC: Cryptographic access control policy
Restrict user access to cryptographic IT assets (e.g., Private keys of users who may share the system) in accordance with a specified user access control policy.

O.Crypto_Key_Man: Cryptographic Key Management
Fully define cryptographic components, functions, and interfaces. Provide the capabilities for distribution, storage, use, and destruction.

O.Crypto_Operation: Cryptographic function definition
Cryptographic interfaces shall be fully defined.

O.Crypto_Test_Reqs: Test cryptographic functionality
Test cryptographic operation and key management before establishing a secure mail application session.

O.Data_Exchange_Conf: Enforce data exchange confidentiality
Provide the ability to protect user data confidentiality.

O.Data_Imp_Exp_Control: Data import/export to/from system control
Protect data from being sent to disallowed places and places in excess of the number allowed by the organization's security policy. Conversely the importation of data into the system should be protected from places not allowed by the organization's security policy.

O.General_Integ_Checks: Periodically check integrity
Provide periodic integrity checks on both the messaging application and user data.

O.I&A: Identify and authenticate a user to support accountability
Associate each transaction between an authenticated user and an application with a unique transaction ID, allowing events associated with a given transaction to be distinguished from other events involving the user and the application.

O.Information_Flow_Control: System enforced information flow
Enforce an information flow policy whereby users are constrained from allowing access to information they control, regardless of their intent (e.g., mandatory access control).

O.Labels: Label or mark information
Label or mark information to prevent the exchange of inappropriate data between users.

O.Limit_Actions_Auth: Restrict actions before authentication
Restrict the actions a user may perform before the TOE verifies the identity of the user.

O.Limit_Mult_Sessions: Limit multiple sessions
Provide the capability to limit the number of mail application sessions that a user may have open at one time.

O.MsgMod_ID: Identify message modification in messages sent or received remotely or locally
The TSF recognizes changes to messages that occurred in transit, including insertion of spurious messages and deletion or replay of legitimate messages.

O.NonRepud_Assess_Recd: Non-repudiation support for received information by a non-local sender's TSF
Support evaluation of non-repudiation evidence by the messaging administrator for received information.

O.NonRepud_Assess_Sent: Non-repudiation support for sent information by the non-local receiving TSF

Support evaluation of non-repudiation evidence by the messaging administrator for sent information.

O.NonRepudiate_Recd: Non-repudiation for received information
Provide evidence to prevent users from avoiding accountability of received messages.

O.NonRepudiate_Sent: Non-repudiation for sent information
Provide evidence to prevent users from avoiding accountability for sending messages to either remotely or locally to another user.

O.Obj_Attr_Integrity: Basic object attribute integrity
Maintain object security attributes with high accuracy. Ensure that security handling (e.g., signatures or encryption) applied to objects remain in effect from origination to receipt of messages.

O.Rollback: Rollback
Recover to a previous known state by undoing user operations (i.e., "rolling back") to restore a previous known state.

O.Security_Attr_Mgt: Manage security attributes
Manage the initialization of, values for, and allowable operations on security attributes.

O.Security_Func_Mgt: Manage behavior of security functions
Provide management mechanisms for security mechanisms.

O.Security_Roles: Security roles
Maintain security-relevant roles and the association of users with those roles.

O.Session_Termination: System terminates session for inactivity
System terminates a session after a given interval of inactivity.

O.Storage_Integrity: Storage integrity
Provide integrity for messages stored by the messaging application

O.User_Attributes: Maintain user attributes
Maintain a set of security attributes (which may include group membership, clearance, access rights, etc.) associated with individual users in addition to user identity.

O.User_Auth_Management: User authorization management
Manage and update user authorization and privilege data in accordance with organizational security and personnel policies.

4.2 Security Objectives for the Environment

O.Audit: Auditing Capabilities
Provide information about past user behavior to an authorized user through system mechanisms to discover system misuse and provide a potential deterrent by warning the user. Auditable actions shall be defined by selection of individual roles. The audit record shall contain date/time of the action, location of the action, and the entity responsible for the action.

O.Clean_Obj_Recovery: Object and data recovery free from malicious code
Recover to a viable state after malicious code is introduced and damage occurs, removing the malicious code as part of the process.

O.Security_Attr_Mgt: Manage security attributes
Manage the initialization of, values for, and allowable operations on security attributes.

O.Security_Func_Mgt: Manage behavior of security functions
Provide management mechanisms for security mechanisms.

O.User_Auth_Management: User authorization management
Manage and update user authorization and privilege data in accordance with organizational security and personnel policies.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

5.1.1 Security Audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the basic level of audit; and

c) Date and time of the event, type of event, subject identity, host identity, message identifier, message location, and the outcome (success or failure) of the event$^{\text{FAU\_GEN.1.1}}$

5.1.1.2 User identity association (FAU_GEN.2)

The TSF shall be able to associate each auditable event with the identity of the user that caused the event.$^{\text{FAU\_GEN.2.1}}$

5.1.1.3 Selective audit (FAU_SEL.1)

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) User identity, subject identity, host identity, event type, destination

b) Date and time of the event, message identifier, message location, and the outcome (success or failure) of the event.$^{\text{FAU\_SEL.1.1}}$

5.1.2 Communication (FCO)

5.1.2.1 Selective proof of origin (FCO_NRO.1)

The TSF shall be able to generate evidence of origin for transmitted messages at the request of the originator.$^{\text{FCO\_NRO.1.1}}$
The TSF shall be able to relate the identity of the originator of the information, and the message content to which the evidence applies.$^{\text{FCO\_NRO.1.2}}$
The TSF shall provide a capability to verify the evidence of origin of information to the recipient.$^{\text{FCO\_NRO.1.3}}$

5.1.2.2 Selective proof of receipt (FCO_NRR.1)

The TSF shall be able to generate evidence of receipt for received messages at the request of the originator.$^{\text{FCO\_NRR.1.1}}$
The TSF shall be able to relate the identity of the recipient and the message to which the evidence applies.$^{\text{FCO\_NRR.1.2}}$

The TSF shall provide a capability to verify the evidence of receipt of the message to the originator.[FCO_NRR.1.3]

5.1.3 Cryptographic Operation (FCS)

5.1.3.1 Cryptographic Operation (FCS_COP.1)

The TSF shall perform encryption in accordance with the specified cryptographic algorithm [ST-assignment: *cryptographic algorithm*] and cryptographic key sizes [ST-assignment: *cryptographic key sizes*] that meet S/MIME version 3 standards. [FCS_COP.1.1]

5.1.4 User Data Protection (FDP)

5.1.4.1 Complete access control (FDP_ACC.2)

The TSF shall enforce mandatory access on individual mail files and server resources, and all operations performed by subjects (i.e., users and messaging administrators) covered by the SFP. [FDP_ACC.2.1]
The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. [FDP_ACC.2.2]

5.1.4.2 Security attribute based access control (FDP_ACF.1)

The TSF shall enforce the mandatory access to objects based on role permissions associated with an authenticated identity.[FDP_ACF.1.1]
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) messaging administrators will be granted full access to messaging resources (2) users will be granted full access to their individual messaging resources (e.g., mailbox, address lists) (3) users will be granted limited access (e.g., Read permission) to shared messaging resources (e.g., Global Address lists, public folders).[FDP_ACF.1.2]

5.1.4.3 Subset information flow control (FDP_IFC.1)

The TSF shall enforce and display sensitivity labels on applicable messages.[FDP_IFC.1.1]

5.1.4.4 Simple security attributes (FDP_IFF.1)

The TSF shall enforce and display sensitivity labels based on the sensitivity label of the originator and recipient.[FDP_IFF.1.1]

5.1.4.5 Import of user data without security attributes (FDP_ITC.1)

The TSF shall enforce the use of sensitivity labels and non-repudiation when importing user data, controlled under the SFP, from outside the TSC.

5.1.4.6 Basic rollback (FDP_ROL.1)

The TSF shall enforce the selection of message protection to permit the rollback of the protection level of the message.[FDP_ROL.1.1]
The TSF shall permit operations to be rolled back.[FDP_ROL.1.2]

5.1.4.7 Basic data exchange confidentiality (FDP_UCT.1)

The TSF shall enforce the access control SFP to be able to transmit and receive messages in a manner protected from unauthorized disclosure.

5.1.4.8 Data exchange integrity (FDP_UIT.1)

The TSF shall be able to protect the integrity of applicable messages. $^{\text{FDP\_UIT.1.1}}$
The TSF shall be able to determine on receipt of user data, whether integrity has been violated. $^{\text{FDP\_UIT.1.2}}$

5.1.5 Identification & Authentication (FIA)

5.1.5.1 User authentication before any action (FIA_UAU.2)

The TSF shall require each user to be strongly authenticated at log-on before allowing any other TSF-mediated actions on behalf of that user.$^{\text{FIA\_UAU.2.1}}$

5.1.5.2 Protected authentication feedback (FIA_UAU.7)

The TSF shall provide limited feedback to the user while the authentication is in progress.$^{\text{FIA\_UAU.7.1}}$

5.1.5.3 Timing of Identification (FIA_UID.1)

The TSF shall allow initiation of the log-in process on behalf of the user before the user is identified.$^{\text{FIA\_UID1.1}}$
The TSF shall require each user to be successfully identified before allowing any other TSF mediated actions on behalf of that user.$^{\text{FIA\_UID1.2}}$

5.1.5.4 User-subject binding (FIA_USB.1)

The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.$^{\text{FIA\_USB.1.1}}$

5.1.6 Security Management (FMT)

5.1.6.1 Management of security functions behavior (FMT_MOF.1)

The TSF shall restrict the ability to determine the behavior of the security functions to the messaging administrator (i.e., users will not be able to change default security settings defined by the messaging administrator).$^{\text{FMT\_MOF.1.1}}$

5.1.6.2 Management of security attributes (FMT_MSA.1)

The TSF shall enforce the policy to restrict the ability to, modify the security attributes to the messaging administrator.$^{\text{FMT\_MSA.1.1}}$

5.1.6.3 Secure security attributes (FMT_MSA.2)

The TSF shall ensure that only secure values are accepted for security attributes.$^{\text{FMT\_MSA.2.1}}$

5.1.6.4 Static attribute initialization (FMT_MSA.3)

The TSF shall enforce the policy to provide restrictive default values (e.g., inbound/outbound routing tables) for security attributes that are used to enforce the SFP.$^{FMT\_MSA.3.1}$
The TSF shall allow the messaging administrator to specify alternative initial values to override the default values when an object or information is created.$^{FMT\_MSA.3.2}$

5.1.6.5 Management of TSF data (FMT_MTD.1)

The TSF shall restrict the ability to change TSF data (e.g., address directory, user authentication information, user accounts, etc.) to the messaging administrator.$^{FMT\_MTD.1.1}$

5.1.6.6 Revocation (FMT_REV.1)

The TSF shall restrict the ability to revoke security attributes associated with the users and objects within the TSC to the messaging administrator.$^{FMT\_REV.1.1}$

5.1.6.7 Security roles (FMT_SMR.1)

The TSF shall maintain the roles of user and messaging administrator.$^{FMT\_SMR.1.1}$
The TSF shall be able to associate users with roles.$^{FMT\_SMR.1.2}$

5.1.7 TOE Access (FTA)

5.1.7.1 Basic limitation on multiple concurrent sessions (FTA_MCS.1)

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.$^{FTA\_MCS.1.1}$

5.1.7.2 TSF-initiated termination (FTA_SSL.3)

The TSF shall terminate an interactive session after a specified time interval assigned by the messaging administrator.$^{FTA\_SSL.3.1}$

5.2 TOE Security Assurance Requirements

Table 5-1 Assurance Requirements: EAL (3)

Assurance Class	Assurance Components
ACM	ACM_CAP.3, ACM_SCP.1
ADO	ADO_DEL.1, ADO_IGS.1
ADV	ADV_FSP.1, ADV_HLD.2, ADV_RCR.1, augmented ADV_SPM.1
AGD	AGD_ADM.1, AGD_USR.1
ALC	ALC_DVS.1

Assurance Class	Assurance Components
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_MSU.1, AVA_SOF.1, AVA_VLA.1

5.2.1 Configuration management (ACM)

5.2.1.1 Authorization controls (ACM_CAP.3)

The CM system shall provide measures such that only authorized changes are made to the configuration items.[ACM_CAP.3.10C]

The reference for the TOE shall be unique to each version of the TOE.[ACM_CAP.3.1C]

The developer shall provide a reference for the TOE.[ACM_CAP.3.1D]

The TOE shall be labeled with its reference.[ACM_CAP.3.2C]

The developer shall use a CM system.[ACM_CAP.3.2D]

The CM documentation shall include a configuration list and a CM plan.[ACM_CAP.3.3C]

The developer shall provide CM documentation.[ACM_CAP.3.3D]

The configuration list shall describe the configuration items that comprise the TOE.[ACM_CAP.3.4C]

The CM documentation shall describe the method used to uniquely identify the configuration items.[ACM_CAP.3.5C]

The CM system shall uniquely identify all configuration items.[ACM_CAP.3.6C]

The CM plan shall describe how the CM system is used.[ACM_CAP.3.7C]

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.[ACM_CAP.3.8C]

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.[ACM_CAP.3.9C]

5.2.1.2 TOE CM coverage (ACM_SCP.1)

The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.[ACM_SCP.1.1C]

The developer shall provide CM documentation.[ACM_SCP.1.1D]

The CM documentation shall describe how configuration items are tracked by the CM system.[ACM_SCP.1.2C]

5.2.2 Delivery and operation (ADO)

5.2.2.1 Delivery procedures (ADO_DEL.1)

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.[ADO_DEL.1.1C]

The developer shall document procedures for delivery of the TOE or parts of it to the user.[ADO_DEL.1.1D]

The developer shall use the delivery procedures.[ADO_DEL.1.2D]

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.[ADO_IGS.1.1C]
The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.[ADO_IGS.1.1D]

5.2.3 Development (ADV)

5.2.3.1 Informal functional specification (ADV_FSP.1)

The functional specification shall describe the TSF and its external interfaces using an informal style.[ADV_FSP.1.1C]
The developer shall provide a functional specification.[ADV_FSP.1.1D]
The functional specification shall be internally consistent.[ADV_FSP.1.2C]
The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.[ADV_FSP.1.3C]
The functional specification shall completely represent the TSF.[ADV_FSP.1.4C]

5.2.3.2 Security enforcing high-level design (ADV_HLD.2)

The presentation of the high-level design shall be informal.[ADV_HLD.2.1C]
The developer shall provide the high-level design of the TSF.[ADV_HLD.2.1D]
The high-level design shall be internally consistent.[ADV_HLD.2.2C]
The high-level design shall describe the structure of the TSF in terms of subsystems.[ADV_HLD.2.3C]
The high-level design shall describe the security functionality provided by each subsystem of the TSF.[ADV_HLD.2.4C]
The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.[ADV_HLD.2.5C]
The high-level design shall identify all interfaces to the subsystems of the TSF.[ADV_HLD.2.6C]
The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.[ADV_HLD.2.7C]
The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.[ADV_HLD.2.8C]
The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems. [ADV_HLD.2.9C]

5.2.3.3 Informal correspondence demonstration (ADV_RCR.1)

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.[ADV_RCR.1.1C]
The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.[ADV_RCR.1.1D]

5.2.3.4 Informal TOE security policy model (ADV_SPM.1)

The TSP model shall be informal.[ADV_SPM.1.1C]
The developer shall provide a TSP model.[ADV_SPM.1.1D]
The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.[ADV_SPM.1.2C]
The developer shall demonstrate correspondence between the functional specification and the TSP model.[ADV_SPM.1.2D]
The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.[ADV_SPM.1.3C]
The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.[ADV_SPM.1.4C]

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

The messaging administrator guidance shall describe the administrative functions and interfaces available to the messaging administrator of the TOE.[AGD_ADM.1.1C]
The developer shall provide messaging administrator guidance addressed to system administrative personnel.[AGD_ADM.1.1D]
The messaging administrator guidance shall describe how to administer the TOE in a secure manner.[AGD_ADM.1.2C]
The messaging administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.[AGD_ADM.1.3C]
The messaging administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.[AGD_ADM.1.4C]
The messaging administrator guidance shall describe all security parameters under the control of the messaging administrator, indicating secure values as appropriate.[AGD_ADM.1.5C]
The messaging administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.[AGD_ADM.1.6C]
The messaging administrator guidance shall be consistent with all other documentation supplied for evaluation.[AGD_ADM.1.7C]
The messaging administrator guidance shall describe all security requirements for the IT environment that are relevant to the messaging administrator.[AGD_ADM.1.8C]

5.2.4.2 User guidance (AGD_USR.1)

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. [AGD_USR.1.1C]
The developer shall provide user guidance.[AGD_USR.1.1D]
The user guidance shall describe the use of user-accessible security functions provided by the TOE.[AGD_USR.1.2C]
The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.[AGD_USR.1.3C]

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.$^{\text{AGD\_USR.1.4C}}$
The user guidance shall be consistent with all other documentation supplied for evaluation.$^{\text{AGD\_USR.1.5C}}$
The user guidance shall describe all security requirements for the IT environment that are relevant to the user.$^{\text{AGD\_USR.1.6C}}$

5.2.5 Life cycle support (ALC)

5.2.5.1 Identification of security measures (ALC_DVS.1)

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.$^{\text{ALC\_DVS.1.1C}}$
The developer shall produce development security documentation.$^{\text{ALC\_DVS.1.1D}}$
The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.$^{\text{ALC\_DVS.1.2C}}$

5.2.6 Tests (ATE)

5.2.6.1 Analysis of coverage (ATE_COV.2)

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.$^{\text{ATE\_COV.2.1C}}$
The developer shall provide an analysis of the test coverage.$^{\text{ATE\_COV.2.1D}}$
The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete. $^{\text{ATE\_COV.2.2C}}$

5.2.6.2 Testing: high-level design (ATE_DPT.1)

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.$^{\text{ATE\_DPT.1.1C}}$
The developer shall provide the analysis of the depth of testing.$^{\text{ATE\_DPT.1.1D}}$

5.2.6.3 Functional testing (ATE_FUN.1)

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.$^{\text{ATE\_FUN.1.1C}}$
The developer shall test the TSF and document the results.$^{\text{ATE\_FUN.1.1D}}$
The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.$^{\text{ATE\_FUN.1.2C}}$
The developer shall provide test documentation.$^{\text{ATE\_FUN.1.2D}}$
The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.$^{\text{ATE\_FUN.1.3C}}$

The expected test results shall show the anticipated outputs from a successful execution of the tests.$^{ATE\_FUN.1.4C}$
The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.$^{ATE\_FUN.1.5C}$

5.2.6.4 Independent testing - sample (ATE_IND.2)

The TOE shall be suitable for testing.$^{ATE\_IND.2.1C}$
The developer shall provide the TOE for testing.$^{ATE\_IND.2.1D}$
The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. $^{ATE\_IND.2.2C}$

5.2.7 Vulnerability assessment (AVA)

5.2.7.1 Examination of guidance (AVA_MSU.1)

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.$^{AVA\_MSU.1.1C}$
The developer shall provide guidance documentation. $^{AVA\_MSU.1.1D}$
The guidance documentation shall be complete, clear, consistent and reasonable.$^{AVA\_MSU.1.2C}$
The guidance documentation shall list all assumptions about the intended environment.$^{AVA\_MSU.1.3C}$
The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).$^{AVA\_MSU.1.4C}$

5.2.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.$^{AVA\_SOF.1.1C}$
The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.$^{AVA\_SOF.1.1D}$
For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.$^{AVA\_SOF.1.2C}$

5.2.7.3 Developer vulnerability analysis (AVA_VLA.1)

The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.$^{AVA\_VLA.1.1C}$
The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.$^{AVA\_VLA.1.1D}$
The developer shall document the disposition of obvious vulnerabilities.$^{AVA\_VLA.1.2D}$

5.3 Security Requirements for the IT Environment

5.3.1 Security Audit (FAU)

5.3.1.1 Audit review (FAU_SAR.1)

The messaging administrators will have the capability to read the audit records of the TOE.[FAU_SAR.1.1]
The audit records will be provided in a format suitable for the messaging administrator to interpret the information. [FAU_SAR.1.2]

5.3.1.2 Selectable audit review (FAU_SAR.3)

The messaging administrators will have the capability to perform searches of the audit records based on definable queries.[FAU_SAR.3.1]

5.3.1.3 Protected audit trail storage (FAU_STG.1)

Stored audit records will be protected from unauthorized deletion.[FAU_STG.1.1]
Stored audit records will be protected in order to prevent and detect unauthorized modifications.[FAU_STG.1.2]

5.3.1.4 Prevention of audit data loss (FAU_STG.4)

When the audit trail is full, the oldest stored audit records will be overwritten and the messaging administrator will be notified.[FAU_STG.4.1]

5.3.2 Protection of the TOE Security Functions (FPT)

5.3.2.1 Abstract Machine Testing (FPT_AMT.1)

The TSF shall run a suite of tests during initial start-up or while invoking the CSP to demonstrate the correct operation of the security assumptions provided by the abstract machine (i.e., cryptographic service provider) that underlies the TSF. [FPT_AMT.1.1]

5.3.2.2 Automated recovery without undue loss (FPT_RCV.3)

When automated recovery from a failure or service discontinuity is not possible, the TOE will enter a maintenance mode where the ability to return to a secure state is provided.[FPT_RCV.3.1]
For messaging application failures, the TOE will return to a secure state using automated procedures.[FPT_RCV.3.2]
The functions provided to recover from failure or service discontinuity will ensure that the secure initial state is restored without exceeding a predefined amount set by the messaging administrator for loss of data or objects within the TOE.[FPT_RCV.3.3]
Objects that were or were not capable of being recovered will be identified. [FPT_RCV.3.4]

6 Rationale

This section presents the evidence used in this Secure Messaging Protection Profile evaluation. This evidence supports the claims that this PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security counter measures within the security environment.

6.1 Security Objectives Rationale

Table 6-1 Mapping the TOE Security Environment to Security Objectives

Policy/Threat/Assumptions	**Objectives**
Security Objectives for the TOE	
P.Accountability	O.Audit, O.I&A, O.NonRepudiate_Recd, O.NonRepudiate_Sent
P.Availability	O.Crypto_Operation, O.Limit_Mult_Sessions, O.User_Auth_Management, O.User_Attributes
P.Information_AC	O.Data_Exchange_Conf, O.Information_Flow_Control, O.Labels, O.Security_Attr_Mgt, O.Security_Func_Mgt
P.Integrity	O.Storage_Integrity, O.Crypto_Operation
P.Lifecycle	O.Apply_Code_Fixes, O.Atomic_Functions, O.Crypto_Operation, O.Crypto_Test_Reqs
P.Marking	O.Labels
T.Admin_Err_Commit	O.Audit, O.Crypto_Key_Man, O.I&A, O.Limit_Actions_Auth, O.Security_Roles
T.Admin_Err_Omit	O.Admin_Guidance, O.AC_Admin_Limit, O.Adm_Limits_Bindings, O.Adm_User_Att_Mod
T.Admin_UserPriv	O.Admin_Guidance, O.AC_Admin_Limit
T.Admin_Hostile_Modify	O.AC_Admin_Limit, O.Adm_Limits_Bindings, O.Adm_User_Att_Mod
T.Component_Failure	O.Crypto_Operation, O.Crypto_Test_Reqs
T.Dev_Flawed_Code	O.Apply_Code_Fixes
T.Failure_DS_Comp	O.Atomic_Functions
T.Hack_AC	O.Apply_Code_Fixes, O.Audit

Policy/Threat/Assumptions	Objectives
Security Objectives for the TOE	
T.Hack_Comm_Eavesdrop	O.Crypto_Operation, O.Data_Exchange_Conf
T.Hack_Masq	O.Session_Termination
T.Hack_Msg_Data	O.MsgMod_ID, O.Crypto_Operation
T.Hack_Social_Engineer	O.Limit_Mult_Sessions
T.Malicious_Code	O.Active_Content, O.Clean_Obj_Recovery, O.General_Integ_Checks
T.Power_Disrupt	O.Atomic_Functions
T.Repudiate_Receive	O.NonRepud_Assess_Recd, O.NonRepudiate_Recd
T.Repudiate_Send	O.NonRepud_Assess_Sent, O.NonRepudiate_Sent,
T.User_Abuse_Conf	O.Data_Exchange_Conf, O.Data_Imp_Exp_Control
T.User_Err_Conf	O.Crypto_AC, O.Labels, O.Data_Imp_Exp_Control
T.User_Err_Inaccess	O.Rollback
T.User_Err_Slf_Protect	O.Obj_Attr_Integrity
T.User_Misuse_Avl_Resc	O.Limit_Mult_Sessions, O.Limit_Actions_Auth, O.Security_Roles, O.User_Attributes, O.User_Auth_Management
T.User_Modify	O.Audit
T.User_Send	O.Audit

Table 6-2 Tracing of Security Objectives to the TOE Security Environment

Objectives	Policy/Threat/Assumptions
Security Objectives for the TOE	
O.AC_Admin_Limit	T.Admin_Hostile_Modify, T.Admin_Err_Omit, T.Admin_UserPriv
O.Active_Content	T.Malicious_Code
O.Adm_Limits_Bindings	T.Admin_Hostile_Modify, T.Admin_Err_Omit
O.Adm_User_Att_Mod	T.Admin_Hostile_Modify, T.Admin_Err_Omit

Objectives	Policy/Threat/Assumptions
Security Objectives for the TOE	
O.Admin_Guidance	T.Admin_Err_Omit, T.Admin_UserPriv
O.Apply_Code_Fixes	T.Hack_AC, P.Lifecycle
O.Atomic_Functions	P.Lifecycle, T.Power_Disrupt, T.Failure_DS_Comp
O.Audit	T.Admin_Err_Commit, T.Hack_AC, P.Accountability, T.User_Modify, T.User_Send
O.Clean_Obj_Recovery	T.Malicious_Code
O.Crypto_AC	T.User_Err_Conf
O.Crypto_Key_Man	T.Admin_Err_Commit
O.Crypto_Operation	T.Component_Failure, T.Hack_Comm_Eavesdrop, T.Hack_Msg_Data, P.Availability, P.Integrity, P.Lifecycle,
O.Crypto_Test_Reqs	T.Component_Failure, P.Lifecycle
O.Data_Exchange_Conf	T.Hack_Comm_Eavesdrop, T.User_Abuse_Conf, P.Information_AC
O.Data_Imp_Exp_Control	T.User_Abuse_Conf, T.User_Err_Conf
O.General_Integ_Checks	T.Malicious_Code
O.I&A	P.Accountability, T.Admin_Err_Commit
O.Information_Flow_Control	P.Information_AC
O.Labels	T.User_Err_Conf, P.Marking, P.Information_AC
O.Limit_Actions_Auth	T.Admin_Err_Commit, T.User_Misuse_Avl_Resc
O.Limit_Mult_Sessions	T.Hack_Social_Engineer, P.Availability, T.User_Misuse_Avl_Resc
O.MsgMod_ID	T.Hack_Msg_Data
O.NonRepud_Assess_Recd	T.Repudiate_Receive
O.NonRepud_Assess_Sent	T.Repudiate_Send
O.NonRepudiate_Recd	P.Accountability, T.Repudiate_Receive
O.NonRepudiate_Sent	P.Accountability, T.Repudiate_Send
O.Obj_Attr_Integrity	T.User_Err_Slf_Protect

Objectives	Policy/Threat/Assumptions
Security Objectives for the TOE	
O.Rollback	T.User_Err_Inaccess
O.Security_Attr_Mgt	P.Information_AC
O.Security_Func_Mgt	P.Information_AC
O.Security_Roles	T.Admin_Err_Commit, T.User_Misuse_Avl_Resc
O.Session_Termination	T.Hack_Masq
O.Storage_Integrity	P.Integrity
O.User_Attributes	T.User_Misuse_Avl_Resc, P.Availability
O.User_Auth_Management	T.User_Misuse_Avl_Resc, P.Availability

6.1.1 Policies

P.Accountability: Individual accountability
Individuals shall be held accountable for their actions.

Coverage Rationale: P.Accountability is established by I&A of the individual, non-repudiation of the individual’s actions, and audit mechanisms used to record their actions.

1. O.Audit: Audit capability
   Provide information about past user behavior to an authorized user through system mechanisms to discover system misuse and provide a potential deterrent by warning the user. Auditable actions shall be defined by selection of individual roles. The audit record shall contain date/time of the action, location of the action, and the entity responsible for the action.
2. O.I&A: Identify and authenticate a user to support accountability
   Associate each transaction between an authenticated user and a system/application with a unique transaction ID, allowing events associated with a given transaction to be distinguished from other events involving the user and/or system/application.
3. O.NonRepudiate_Recd: Non-repudiation for received information
   Provide evidence to prevent users from avoiding accountability of received messages.
4. O.NonRepudiate_Sent: Non-repudiation for sent information
   Provide evidence that a user sent information.

P.Availability: Information availability
Information shall be available to satisfy mission requirements.

Coverage Rationale: P.Availability is provided by cryptographic functions protecting sensitive information and limiting the misuse of resources.

1. O.Crypto_Operation: Cryptographic function definition
   Cryptographic components, functions, and interfaces shall be fully defined.

2. O.Limit_Mult_Sessions: Limit multiple sessions
   Provide the capability to limit the number of sessions that a user may have open at one time.

3. O.User_Auth_Management: User authorization management
   Manage and update user authorization and privilege data in accordance with organizational security and personnel policies.

4. O.User_Attributes: Maintain user attributes
   Maintain a set of security attributes (which may include group membership, clearance, access rights, etc.) associated with individual users in addition to user identity.

P.Information_AC: Information access control
Information shall be accessed only by authorized individuals and processes.

Coverage Rationale: P.Information_AC is enforced by the role and permissions of the individuals.

1. O.Data_Exchange_Conf: Enforce data exchange confidentiality
   Protect user data confidentiality when exchanging data with a remote system.

2. O.Information_Flow_Control: System enforced information flow
   Enforce an information flow policy whereby users are constrained from allowing access to information they control, regardless of their intent (e.g., mandatory access control).

3. O.Labels: Label or mark information
   Label or mark information to prevent the exchange of inappropriate data between users.

4. O.Security_Attr_Mgt: Manage security attributes
   Manage the initialization of, values for, and allowable operations on security attributes.

5. O.Security_Func_Mgt: Manage behavior of security functions
   Provide management mechanisms for security mechanisms.

P.Integrity: Information content integrity
Information shall retain its content integrity.

Coverage Rationale: P.Integrity protects information against modification through cryptographic methods.

1. O.Storage_Integrity: Storage integrity
   Provide integrity for data.

2. O.Crypto_Operation: Cryptographic function definition
   Cryptographic components, functions, and interfaces shall be fully defined.

P.Lifecycle: System lifecycle phases integrate security
Information systems security shall be an integral part of system lifecycle phases of design, development and integration. Installation, restoration, update, and removal

phases may integrate security procedures and options only to the extent provided by the messaging application design.

Coverage Rationale: P.Lifecycle ensures that the messaging application is complete and functions correctly.

1. O.Apply_Code_Fixes: Apply patches to fix the code
   Apply patches to fix the code when vulnerabilities in code allow unauthorized and undiscovered access.
2. O.Atomic_Functions: Complete the security functions or recover to previous state
   Recover automatically to a consistent, secure state if a security function does not successfully complete in the presence of certain types of failures.
3. O.Crypto_Operation: Cryptographic function definition
   Cryptographic components, functions, and interfaces shall be fully defined.
4. O.Crypto_Test_Reqs: Test cryptographic functionality
   Test cryptographic operation and key management.

P.Marking: Information marking
Information shall be appropriately marked and labeled.

Coverage Rationale: P.Marking provides for the capability to label information.

1. O.Labels: Label or mark information
   Label or mark information to prevent the exchange of inappropriate data between users.

6.1.2 Threats

T.Admin_Err_Commit: Administrative errors of commission
A messaging administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application.

Coverage Rationale: T.Admin_Err_Commit is addressed by:

1. O.Audit: Auditing for user accountability
   Provide information about past user behavior to an authorized user through system mechanisms to discover system misuse and provide a potential deterrent by warning the user. Auditable actions shall be defined by selection of individual roles. The audit record shall contain date/time of the action, location of the action, and the entity responsible for the action.
2. O.Crypto_Key_Man: Cryptographic Key Management
   Fully define cryptographic components, functions, and interfaces. Ensure appropriate protection for cryptographic keys throughout their lifecycle, covering generation, distribution, storage, use, and destruction.
3. O.I&A: Identify and authenticate a user to support accountability
   Associate each transaction between an authenticated user and an application with

a unique transaction ID, allowing events associated with a given transaction to be distinguished from other events involving the user and the application.

4. O.Limit_Actions_Auth: Restrict actions before authentication
   Restrict the actions a user may perform before the TOE verifies the identity of the user.
5. O.Security_Roles: Security roles
   Maintain security-relevant roles and the association of users with those roles.

T.Admin_Hostile_Modify: Hostile administrator modification of user or system data
A messaging administrator maliciously obstructs organizational security objectives or modifies the system's configuration to allow security violations to occur.

Coverage Rationale: T.Admin_Hostile_Modify is addressed by:

1. O.AC_Admin_Limit: Limitation of administrative access control
   Design administrative functions in such a way that the messaging administrators do not automatically have access to user objects (i.e., user accounts), except for necessary exceptions.
2. O.Adm_Limits_Bindings: Limit a messaging administrator's ability to modify user-subject bindings
   Limit the messaging administrator from modification of user-subject bindings in an effort to deter messaging administrators and users from acting without accountability.
3. O.Adm_User_Att_Mod: Limit the messaging administrator's modification of user attributes
   Deter the messaging administrator from maliciously modifying users' attributes. Such modifications could allow unauthorized user actions or denial of service to a legitimate user.

T.Admin_Err_Omit: Administrative errors of omission
The messaging administrator fails to perform some function essential to security

Coverage Rationale: T.Admin_Err_Omit is addressed by:

1. O.Admin_Guidance: Administrator guidance documentation
   Deter messaging administrator errors by providing adequate messaging administrator guidance.
2. O.AC_Admin_Limit: Limitation of administrative access control
   Design administrative functions in such a way that the messaging administrators do not automatically have access to user objects (i.e., user accounts), except for necessary exceptions.
3. O.Adm_Limits_Bindings: Limit an administrator's ability to modify user-subject bindings
   Limit the messaging administrator from modification of user-subject bindings in an effort to deter messaging administrators and users from acting without accountability.

4. O.Adm_User_Att_Mod: Limit administrator's modification of user attributes
   Deter the messaging administrator from maliciously modifying users' attributes. Such modifications could allow unauthorized user actions or denial of service to a legitimate user.

T.Admin_UserPriv: Administrator violates user privacy policy
Messaging administrator may have full operating system access privileges, which would allow for the disclosure of privacy-related information, which is sensitive information associated with the identity of a user. Prevention of messaging administrator abuses by an application is not possible. Messaging administrator may be constrained by role within the messaging application process space.

Coverage Rationale: T.Admin_UserPriv is addressed by:

1. O.Admin_Guidance: Administrator guidance documentation
   Deter messaging administrator errors by providing adequate messaging administrator guidance.
2. O.AC_Admin_Limit: Limitation of administrative access control
   Design administrative functions in such a way that the messaging administrators do not automatically have access to user objects (i.e., user accounts), except for necessary exceptions.

T.Component_Failure: A critical system component fails

Failure of one or more system components results in the loss of system-critical functionality.

Coverage Rationale: T.Component_Failure is addressed by:

1. O.Crypto_Operation: Cryptographic function definition
   Cryptographic components, functions, and interfaces shall be fully defined.
2. O.Crypto_Test_Reqs: Test cryptographic functionality
   Test cryptographic operation and key management.

T.Dev_Flawed_Code: Software containing security-related flaws
A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

Coverage Rationale: T.Dev_Flawed_Code is addressed by:

1. O.Apply_Code_Fixes: Apply patches to fix the code
   Apply patches to fix the code when vulnerabilities in code allow unauthorized and undiscovered access.

T.Failure_DS_Comp Failure of a distributed system component
Failure of a component that is part of a distributed system will cause other parts of the distributed system to malfunction or provide unreliable results.

Coverage Rationale: T.Failure_DS_Comp is addressed by:

1. O.Atomic_Functions: Complete security functions or recover to previous state
   Recover automatically to a consistent, secure state if a security function does not complete successfully in the presence of certain types of failures.

T.Hack_AC: Hacker undetected system access
A hacker gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

Coverage Rationale: T.Hack_AC is addressed by:

1. O.Apply_Code_Fixes: Apply patches to fix the code
   Apply patches to fix the code when vulnerabilities in code allow unauthorized and undiscovered access.
2. O.Audit: Auditing for user accountability
   Provide information about past user behavior to an authorized user through system mechanisms to discover system misuse and provide a potential deterrent by warning the user. Auditable actions shall be defined by selection of individual roles. The audit record shall contain date/time of the action, location of the action, and the entity responsible for the action.

T.Hack_Comm_Eavesdrop: Hacker eavesdrops on user data communications
Hacker obtains user data by eavesdropping on communications lines.

Coverage Rationale: T.Hack_Comm_Eavesdrop is addressed by:

1. O.Crypto_Operation: Cryptographic function definition
   Cryptographic components, functions, and interfaces shall be fully defined.
2. O.Data_Exchange_Conf: Enforce data exchange confidentiality
   Protect user data confidentiality when exchanging data with a remote system

T.Hack_Masq: Hacker masquerading as a legitimate user or as system process
A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process.

Coverage Rationale: T.Hack_Masq is addressed by:

1. O.Session_Termination: System terminates session for inactivity
   System terminates a session after a given interval of inactivity.

T.Hack_Msg_Data: Message content modification
A hacker modifies information intercepted from a communication link between two unsuspecting entities before passing it on, thereby deceiving the intended recipient.

Coverage Rationale: T.Hack_Msg_Data is addressed by:

1. O.Crypto_Operation: Cryptographic function definition
   Cryptographic components, functions, and interfaces shall be fully defined.
2. O.MsgMod_ID: Identify message modification in messages sent or received remotely or locally
   The TSF recognizes changes to messages that occurred in transit, including insertion of spurious messages and deletion or replay of legitimate messages.

T.Hack_Social_Engineer: Social engineering
A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

Coverage Rationale: T.Hack_Social_Engineer is addressed by:

1. O.Limit_Mult_Sessions: Limit multiple sessions
   Provide the capability to limit the number of sessions that a user may have open at one time.

T.Malicious_Code: Malicious code exploitation
An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of system assets.

Coverage Rationale: T.Malicious_Code is addressed by:

1. O.Active_Content: Limit active content capability
   Selection by the client application to active/deactivate active content execution in order to deter embedded malicious code
2. O.Clean_Obj_Recovery: Object and data recovery free from malicious code
   Recover to a viable state after malicious code is introduced and damage occurs, removing the malicious code as part of the process.
3. O.General_Integ_Checks: Periodically check integrity
   Provide periodic integrity checks on both system and user data.

T.Power_Disrupt: Unexpected disruption of system or component power
A human or environmental agent disrupts power causing the system to lose information or security protection.

Coverage Rationale: T.Power_Disrupt is addressed by:

1. O.Atomic_Functions: Complete security functions or recover to previous state
   Recover automatically to a consistent, secure state if a security function does not complete successfully in the presence of certain types of failures.

T.Repudiate_Receive: Recipient denies receiving information
The recipient of a message denies receiving the message, to avoid accountability for receiving the message or to avoid obligations incurred as a result of receiving the message.

Coverage Rationale: T.Repudiate_Receive is addressed by:

1. O.NonRepud_Assess_Recd: Non-repudiation support for received information by a non-local sender's TSF. Support non-repudiation for received information by supporting remote handling of non-repudiation evidence if needed.
2. O.NonRepudiate_Recd: Non-repudiation for received information
   Provide evidence to prevent users from avoiding accountability of received messages.

T.Repudiate_Send: Sender denies sending information
The sender of a message denies sending the message to avoid accountability for sending the message or to avoid obligations incurred as a result of sending the message.

Coverage Rationale: T.Repudiate_Send is addressed by:

1. O.NonRepud_Assess_Sent: Non-repudiation support for sent information by the non-local receiving TSF. Support non-repudiation for sent information by supporting remote handling of non-repudiation evidence.
2. O.NonRepudiate_Sent: Non-repudiation for sent information
   Provide evidence to prevent users from avoiding accountability for sending messages to either remotely or locally to another user.

T.User_Abuse_Conf: Hostile user acts cause confidentiality breaches
A user collects sensitive or proprietary information and removes it from the system.

Coverage Rationale: T.User_Abuse_Conf is addressed by:

1. O.Data_Imp_Exp_Control: Data import/export to/from system control
   Protect data from being sent to disallowed places and places in excess of the number allowed by the organization's security policy. Conversely the importation of data into the system should be protected from places not allowed by the organization's security policy.
2. O.Data_Exchange_Conf: Enforce data exchange data confidentiality
   Provide the ability to protect user data confidentiality.

T.User_Err_Conf: User errors cause confidentiality breaches
A user commits errors that cause information to be delivered to the wrong place or wrong person.

Coverage Rationale: T.User_Err_Conf is addressed by:

1. O.Crypto_AC: Cryptographic access control policy
   Restrict user access to cryptographic IT assets (e.g., Private keys of users who may share the system) in accordance with a specified user access control policy.
2. O.Labels: Label or mark information
   Label or mark information to prevent the exchange of inappropriate data between users.
3. O.Data_Imp_Exp_Control: Data import/export to/from system control
   Protect data from being sent to disallowed places and places in excess of the number allowed by the organization's security policy. Conversely the importation of data into the system should be protected from places not allowed by the organization's security policy.

T.User_Err_Inaccess: User error makes data inaccessible
A user accidentally deletes user data or changes system data rendering user data inaccessible.

Coverage Rationale: T.User_Err_Inaccess is addressed by:

1. O.Rollback: Rollback
   Recover from user operations by undoing some user operations (i.e., "rolling back") to restore a previous known state.

T.User_Err_Slf_Protect: User errors undermine the system's security features
A user commits errors that cause the system or one of its applications to undermine the system's security features.

Coverage Rationale: T.User_Err_Slf_Protect is addressed by:

1. O.Obj_Attr_Integrity: Basic object attribute integrity
   Maintain object security attributes with moderate to high accuracy (under the guidance of qualified users).

T.User_Misuse_Avl_Resc: User's misuse causes denial of service
A user's unauthorized use of resources causes an undue burden on an affected resource.

Coverage Rationale: T.User_Misuse_Avl_Resc is addressed by:

1. O.Limit_Actions_Auth: Restrict actions before authentication
   Restrict the actions a user may perform before the TOE verifies the identity of the user.
2. O.Limit_Mult_Sessions: Limit multiple sessions
   Provide the capability to limit the number of sessions that a user may have open at one time.
3. O.Security_Roles: Security roles
   Maintain security-relevant roles and the association of users with those roles.
4. O.User_Attributes: Maintain user attributes
   Maintain a set of security attributes (which may include group membership, clearance, access rights, etc.) associated with individual users in addition to user identity.
5. O.User_Auth_Management: User authorization management
   Manage and update user authorization and privilege data in accordance with organizational security and personnel policies.

T.User_Modify: User abuses authorization to modify data
A user abuses granted authorizations to improperly change or destroy sensitive or security-critical data.

Coverage Rationale: T.User_Modify is addressed by:

1. O.Audit: Audit capability
   Provide information about past user behavior to an authorized user through system mechanisms to discover system misuse and provide a potential deterrent by warning the user. Auditable actions shall be defined by selection of individual roles. The audit record shall contain date/time of the action, location of the action, and the entity responsible for the action.

T.User_Send: User abuses authorization to send data
A user abuses granted authorizations to improperly send sensitive or security-critical data.

Coverage Rationale: T.User_Send is addressed by:

1. O.Audit: Audit capability
   Provide information about past user behavior to an authorized user through system mechanisms to discover system misuse and provide a potential deterrent by warning the user. Auditable actions shall be defined by selection of individual roles. The audit record shall contain date/time of the action, location of the action, and the entity responsible for the action.

6.2 Security Requirements Rationale

6.2.1 Functional Security Requirements Rationale

Table 6-3 Functional Component to Security Objective Mapping

Objectives	Requirements
O.AC_Admin_Limit	FDP_ACF.1, FDP_ACC.2
O.Active_Content	FDP_UIT.1
O.Adm_Limits_Bindings	FIA_UAU.2, FIA_USB.1, FMT_MTD.1
O.Adm_User_Att_Mod	FAU_GEN.1, FAU_GEN.2, FIA_UAU.2, FMT_MSA.1
O.Admin_Guidance	ACM_SCP.1, ADO_DEL.1, ADO_IGS.1, ADV_HLD.2, AGD_ADM.1, ALC_DVS.1, AVA_MSU.1
O.Apply_Code_Fixes	ACM_CAP.3, ACM_SCP.1, ADO_DEL.1, ADO_IGS.1, ADV_HLD.2, AGD_ADM.1, ALC_DVS.1, FMT_MOF.1, FMT_MSA.1
O.Atomic_Functions	ADV_HLD.2, FPT_RCV.3
O.Audit	FAU_GEN.1, FAU_GEN.2, FAU_SAR.3, FAU_SEL.1, FMT_MOF.1, FMT_SMR.1,FAU_STG.4, FAU_STG.1
O.Clean_Obj_Recovery	FDP_ROL.1, FMT_MOF.1
O.Crypto_AC	FDP_ACC.2, FDP_ACF.1
O.Crypto_Key_Man	ADV_FSP.1, ADV_RCR.1, ADV_SPM.1, AVA_VLA.1, FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MTD.1
O.Crypto_Operation	ACM_CAP.3, ACM_SCP.1, ADV_FSP.1, ADV_HLD.2, ADV_RCR.1, ADV_SPM.1, ALC_DVS.1

Objectives	Requirements
O.Crypto_Test_Reqs	ADV_HLD.2, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, AVA_SOF.1, AVA_VLA.1, FPT_AMT.1
O.Data_Exchange_Conf	FCS_COP.1,FDP_ACC.2, FDP_ITC.1,FDP_UCT.1,ACM_CAP.3
O.Data_Imp_Exp_Control	FMT_MSA.3
O.General_Integ_Checks	FDP_UIT.1
O.I&A	FIA_UAU.2, FIA_UAU.7, FIA_USB.1, AGD_ADM.1, AGD_USR.1, FIA_UID.1, FMT_MOF.1
O.Information_Flow_Control	FDP_IFF.1
O.Labels	FDP_IFC.1, FDP_IFF.1
O.Limit_Actions_Auth	FIA_UAU.2
O.Limit_Mult_Sessions	FTA_MCS.1
O.NonRepud_Assess_Recd	AGD_ADM.1, AGD_USR.1, FCO_NRR.1, FMT_MOF.1
O.NonRepud_Assess_Sent	AGD_ADM.1, AGD_USR.1, FCO_NRO.1, FMT_MOF.1
O.NonRepudiate_Sent	AGD_ADM.1, AGD_USR.1, FCO_NRO.1 FMT_MOF.1
O.NonRepudiate_Recd	AGD_ADM.1, AGD_USR.1, FCO_NRR.1 FMT_MOF.1
O.Obj_Attr_Integrity	FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMR.1
O.MsgMod_ID	FDP_UIT.1
O.Rollback	FDP_ROL.1
O.Security_Attr_Mgt	FMT_MSA.1, FMT_MSA.2, FMT_MSA.3
O.Security_Func_Mgt	FMT_MOF.1
O.Security_Roles	FMT_SMR.1
O.Session_Termination	FTA_SSL.3
O.Storage_Integrity	FMT_MTD.1, FDP_UIT.1

Objectives	Requirements
O.User_Attributes	FDP_ACC.2, FDP_ACF.1, FMT_MSA.2, FMT_MSA.3, FMT_SMR.1, FMT_REV.1
O.User_Auth_Management	AGD_ADM.1, AGD_USR.1, FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMR.1, FMT_REV.1

O.AC_Admin_Limit: Limitation of administrative access control
Design administrative functions in such a way that the messaging administrators do not automatically have access to user objects (i.e., user accounts), except for necessary exceptions.

O.AC_Admin_Limit is implemented in the TOE by:

1. FDP_ACF.1: Security attribute based access control

2. FDP_ACC.2: Complete access control

O.Active_Content: Limit active content capability
Selection by the client application to active/deactivate active content detection in order to deter embedded malicious code within executable files.

O.Active_Content is implemented in the TOE by:

1. FDP_UIT.1: Data exchange integrity

O.Adm_Limits_Bindings: Limit an administrator's ability to modify user-subject bindings
Limit the messaging administrator from modification of user-subject bindings in an effort to deter messaging administrators and users from acting without accountability.

O.Adm_Limits_Bindings is implemented in the TOE by:

1. FIA_UAU.2: User authentication before any action

2. FIA_USB.1: User-subject binding

3. FMT_MTD.1: Management of TSF data

O.Adm_User_Att_Mod: Limit administrator's modification of user attributes
Deter the messaging administrator from maliciously modifying users' attributes. Such modifications could allow unauthorized user actions or denial of service to a legitimate user.

O.Adm_User_Att_Mod is implemented in the TOE by:

1. FAU_GEN.1: Audit data generation

2. FAU_GEN.2: User identity association

3. FIA_UAU.2: User authentication before any action

4. FMT_MSA.1: Management of security attributes

O.Admin_Guidance: Administrator guidance documentation
Deter messaging administrator errors by providing adequate messaging administrator guidance.

O.Admin_Guidance is implemented in the TOE by:

1. ACM_SCP.1: TOE CM coverage

2. ADO_DEL.1: Delivery procedures

3. ADO_IGS.1: Installation, generation, and start-up procedures

4. ADV_HLD.2: Security enforcing high-level design

5. AGD_ADM.1: Administrator guidance

6. ALC_DVS.1: Identification of security measures

7. AVA_MSU.1: Examination of guidance

O.Apply_Code_Fixes: Apply patches to fix the code
Apply patches to fix the code when vulnerabilities in code allow unauthorized and undiscovered access.

O.Apply_Code_Fixes is implemented in the TOE by:

1. ACM_CAP.3 Authorization controls

2. ACM_SCP.1 TOE CM coverage

3. ADO_DEL.1 Delivery procedures

4. ADO_IGS.1 Installation, generation, and start-up procedures

5. ADV_HLD.2 Security enforcing high-level design

6. AGD_ADM.1: Administrator guidance

7. ALC_DVS.1: Identification of security measures

8. FMT_MOF.1: Management of security functions behavior

9. FMT_MSA.1: Management of security attributes

O.Atomic_Functions: Complete security functions or recover to previous state
Recover automatically to a consistent, secure state if a security function does not complete successfully in the presence of certain types of failures.

O.Atomic_Functions is implemented in the TOE by:

1. ADV_HLD.2: Security enforcing high-level design

2. FPT_RCV.3 Automated recovery without undue loss

O.Audit: Auditing for user accountability
Provide information about past user behavior to an authorized user through system mechanisms to discover system misuse and provide a potential deterrent by warning the user. Auditable actions shall be defined by selection of individual roles. The audit record shall contain date/time of the action, location of the action, and the entity responsible for the action.

O.Audit is implemented in the TOE by:

1. FAU_GEN.1: Audit data generation

2. FAU_GEN.2: User identity association

3. FAU_SAR.3: Selectable audit review

4. FAU_SEL.1: Selective audit

5. FMT_MOF.1: Management of security functions behavior

6. FMT_SMR.1: Security roles

O.Clean_Obj_Recovery: Object and data recovery free from malicious code
Recover to a viable state after malicious code is introduced and damage occurs, removing the malicious code as part of the process.

O.Clean_Obj_Recovery is implemented in the TOE by:

1. FDP_ROL.1: Basic rollback

2. FMT_MOF.1: Management of security functions behavior

O.Crypto_AC: Cryptographic access control policy
Restrict user access to cryptographic IT assets in accordance with a specified user access control policy.

O.Crypto_AC is implemented in the TOE by:

1. FDP_ACC.2: Complete access control

2. FDP_ACF.1: Security attribute based access control

O.Crypto_Key_Man: Cryptographic Key Management
Fully define cryptographic components, functions, and interfaces. Ensure appropriate protection for cryptographic keys throughout their lifecycle, covering generation, distribution, storage, use, and destruction.

O.Crypto_Key_Man is implemented in the TOE by:

1. ADV_FSP.1: Informal functional specification

2. ADV_RCR.1: Informal correspondence demonstration

3. ADV_SPM.1: Informal TOE security policy model.

4. AVA_VLA.1: Developer vulnerability analysis

5. FDP_ACC.2: Complete access control

6. FDP_ACF.1: Security attribute based access control

7. FMT_MSA.1: Management of security attributes

8. FMT_MTD.1: Management of TSF data

O.Crypto_Operation: Cryptographic function definition
Cryptographic components, functions, and interfaces shall be fully defined.

O.Crypto_Operation is implemented in the TOE by:

1. ACM_CAP.3: Authorization controls

2. ACM_SCP.1: TOE CM coverage

3. ADV_FSP.1: Informal functional specification

4. ADV_HLD.2: Security enforcing high-level design

5. ADV_RCR.1: Informal correspondence demonstration

6. ADV_SPM.1: Informal TOE security policy model

7. ALC_DVS.1: Identification of security measures

O.Crypto_Test_Reqs: Test cryptographic functionality
Test cryptographic operation and key management.

O.Crypto_Test_Reqs is implemented in the TOE by:

1. ADV_HLD.2: Security enforcing high-level design

2. ATE_COV.2: Analysis of coverage

3. ATE_DPT.1: Testing: high-level design

4. ATE_FUN.1: Functional testing

5. ATE_IND.2: Independent testing - sample

6. AVA_SOF.1: Strength of TOE security function evaluation

7. AVA_VLA.1: Developer vulnerability analysis.

8. FPT_AMT.1: Abstract machine testing

O.Data_Exchange_Conf: Enforce data exchange confidentiality
Provide the ability to protect user data confidentiality.

O.Data_Exchange_Conf is implemented in the TOE by:

1. FCS_COP.1 Cryptographic operation
2. FDP_ACC.2 Complete access control
3. FDP_ITC.1 Import of user data without security attributes
4. FDP_UCT.1 Basic data exchange confidentiality
5. ACM_CAP.3 Authorization controls

O.Data_Imp_Exp_Control: Data import/export to/from system control
Protect data from being sent to disallowed places and places in excess of the number allowed by the organization's security policy. Conversely the importation of data into the system should be protected from places not allowed by the organization's security policy.

O.Data_Imp_Exp_Control is implemented in the TOE by:

1. FMT_MSA.3: Static attribute initialization

O.General_Integ_Checks: Periodically check integrity
Provide periodic integrity checks on both system and user data.

O.General_Integ_Checks is implemented in the TOE by:

1. FDP_UIT.1: Data exchange integrity

O.Labels: Label or mark information
Label or mark information to prevent the exchange of inappropriate data between users.

O.Labels is implemented in the TOE by:

1. FDP_IFC.1: Subset information flow control

2. FDP_IFF.1: Simple security attributes

O.I&AIdentify and authenticate a user to support accountability
Associate each transaction between an authenticated user and a system/application with a unique transaction ID, allowing events associated with a given transaction to be distinguished from other events involving the user and/or system/application.

O.I&A is implemented in the TOE by:

1. FIA_UAU.2: User authentication before any action

2. FIA_UAU.5: Multiple authentication mechanisms

3. FIA_UAU.7: Protected authentication feedback

4. FIA_USB.1: User-subject binding

5. AGD_ADM.1: Administrator guidance

6. AGD_USR.1: User guidance

7. FIA_UID.1: Timing of identification

8. FIA_USB.1: User-subject binding

9. FMT_MOF.1: Management of security functions behavior

O.Information_Flow_Control: System enforced information flow
Enforce an information flow policy whereby users are constrained from allowing access to information they control, regardless of their intent (e.g., mandatory access control).

O.Information_Flow_Control is implemented in the TOE by:

1. FDP_IFF.1: Simple security attributes

O.Limit_Actions_Auth: Restrict actions before authentication
Restrict the actions a user may perform before the TOE verifies the identity of the user.

O.Limit_Actions_Auth is implemented in the TOE by:

1. FIA_UAU.2: User authentication before any action

O.Limit_Mult_Sessions: Limit multiple sessions
Provide the capability to limit the number of sessions that a user may have open at one time.

O.Limit_Mult_Sessions is implemented in the TOE by:

1. FTA_MCS.1: Basic limitation on multiple concurrent sessions

O.MsgMod_ID: Identify message modification in messages sent or received remotely or locally
The TSF recognizes changes to messages that occurred in transit, including insertion of spurious messages and deletion or replay of legitimate messages.

O.MsgMod_ID is implemented in the TOE by:

1. FDP_UIT.1: Data exchange integrity

O.NonRepud_Assess_Recd Non-repudiation support for received information by a non-local sender's TSF
Support non-repudiation for received information by supporting remote handling of non-repudiation evidence if needed.

O.NonRepud_Assess_Recd is implemented in the TOE by:

1. AGD_ADM.1: Administrator guidance

2. AGD_USR.1: User guidance

3. FCO_NRR.1: Selective proof of receipt

4. FMT_MOF.1: Management of security functions behavior

O.NonRepud_Assess_Sent; Non-repudiation support for sent information by the non-local receiving TSF
Support non-repudiation for sent information by supporting remote handling of non-repudiation evidence.

O.NonRepudiate_Sent is implemented in the TOE by:

1. AGD_ADM.1: Administrator guidance

2. AGD_USR.1: User guidance

3. FCO_NRO.1: Selective proof of origin

4. FMT_MOF.1: Management of security functions behavior

O.NonRepudiate_Recd: Non-repudiation for received information
Provide evidence to prevent users from avoiding accountability of received messages.

O.NonRepudiate_Recd is implemented in the TOE by:

1. AGD_ADM.1: Administrator guidance

2. AGD_USR.1: User guidance

3. FCO_NRR.1: Selective proof of receipt

4. FMT_MOF.1: Management of security functions behavior

O.NonRepudiate_Sent: Non-repudiation for sent information
Provide evidence to prevent users from avoiding accountability for sending messages to either remotely or locally to another user.

O.NonRepudiate_Sent is implemented in the TOE by:

1. AGD_ADM.1: Administrator guidance

2. AGD_USR.1: User guidance

3. FCO_NRO.1: Selective proof of origin

4. FMT_MOF.1: Management of security functions behavior

O.Obj_Attr_Integrity: Basic object attribute integrity
Maintain object security attributes with moderate to high accuracy (under the guidance of qualified users). Ensure that security handling (i.e., signed or encrypted) applied to objects remain in affect from origination to receipt of messages.

O.Obj_Attr_Integrity is implemented in the TOE by:

1. FDP_ACC.2: Complete access control

2. FDP_ACF.1: Security attribute based access control

3. FMT_MSA.1: Management of security attributes

4. FMT_MSA.2: Secure security attributes

5. FMT_MSA.3: Static attribute initialization

6. FMT_SMR.1: Security roles

O.Rollback: Rollback
Recover from user operations by undoing some user operations (i.e., "rolling back") to restore a previous known state.

O.Rollback is implemented in the TOE by:

1. FDP_ROL.1: Basic rollback

O.Security_Attr_Mgt: Manage security attributes
Manage the initialization of, values for, and allowable operations on security attributes.

O.Security_Attr_Mgt is implemented in the TOE by:

1. FMT_MSA.1: Management of security attributes

2. FMT_MSA.2: Secure security attributes

3. FMT_MSA.3: Static attribute initialization

O.Security_Func_Mgt: Manage behavior of security functions
Provide management mechanisms for security mechanisms.

O.Security_Func_Mgt is implemented in the TOE by:

1. FMT_MOF.1: Management of security functions behavior

O.Security_Roles: Security roles
Maintain security-relevant roles and the association of users with those roles.

O.Security_Roles is implemented in the TOE by:

1. FMT_SMR.1: Security roles

O.Session_Termination: System terminates session for inactivity
System terminates a session after a given interval of inactivity.

O.Session_Termination is implemented in the TOE by:

1. FTA_SSL.3: TSF-initiated termination

O.Storage_Integrity: Storage integrity
Provide integrity for data.

O.Storage_Integrity is implemented in the TOE by:

1. FDP_UIT.1: Data exchange integrity

2. FMT_MTD.1: Management of TSF Data

O.User_Auth_Management User authorization management
Manage and update user authorization and privilege data in accordance with organizational security and personnel policies.

O.User_Auth_Management is implemented in the TOE by:

1. AGD_ADM.1: Administrator guidance

2. AGD_USR.1: User guidance

3. FMT_MSA.1: Management of security attributes

4. FMT_MSA.2: Secure security attributes

5. FMT_MSA.3: Static attribute initialization

6. FMT_REV.1: Revocation

7. FMT_SMR.1: Security roles

8. FDP_ACC.2: Complete access control

9. FDP_ACF.1: Security attribute based access control

6.2.2 Assurance Security Requirements Rationale

The assurance requirements selected (Table 5.1) to support the functional security requirements (Table 6-4) for this Secure Messaging Protection Profile all mapped to the EAL 3 augmented with ADV_SPM.1. Therefore EAL 3 is appropriate for this PP.

6.3 Dependency Rationale

Table 6-4 Functional and Assurance Requirements Dependencies

Requirement	Dependencies
Functional Requirements	
FAU_SAR.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1

Requirement	Dependencies
Functional Requirements	
FAU_GEN.2	FAU_GEN.1, FIA_UID.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1
FAU_STG.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1
FCS_COP.1	FDP_ITC.1, FMT_MSA.2
FDP_ACC.2	FDP_ACF.1
FDP_ACF.1	FMT_MSA.3
FDP_IFC.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3
FDP_ROL.1	FDP_IFC.1
FDP_UCT.1	FDP_IFC.1
FDP_UIT.1	FDP_IFC.1, FTP_ITC.1
FIA_UAU.2	FIA_UID.1
FMT_MOF.1	FMT_SMR.1
FMT_MSA.1	FDP_IFC.1, FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, FDP_IFC.1, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1
FMT_REV.1	FMT_SMR.1
FPT_RCV.3	AGD_ADM.1, ADV_SPM.1, FPT_TST.1
Assurance Requirements	
ACM_CAP.3	ACM_SCP.1, ALC_DVS.1
ACM_SCP.1	ACM_CAP.3
ADO_IGS.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1

Requirement	**Dependencies**
Functional Requirements	
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1
ADV_SPM.1	ADV_FSP.1
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ATE_COV.2	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	ATE_FUN.1
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.1	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	ADV_FSP.1
AVA_VLA.1	ADV_FSP.1, AGD_ADM.1, AGD_USR.1

Table 6-5 Justification of Unsupported Dependencies

Unsupported Dependencies	**Rationale**
Functional Requirements	
FCS_CKM.1 & FCS_CKM.4	FCS_COP.1 does not require the dependencies FCS_CKM.1 & FCS_CKM.4 within this profile because cryptographic keys are outside the scope of this profile.
FDP_ACC.1	FDP_ACF.1 no longer requires the FDP_ACC.1 dependency because the application will enforce complete access control (FDP_ACC.2) instead of subset access control.
FIA_ATD.1	FIA_USB.1 no longer requires the FIA_ATD.1 dependency because the application does not store user security attributes.

Unsupported Dependencies	Rationale
Functional Requirements	
FIA_UAU.1	FIA_UAU.7 does not require the dependency FIA_UAU.1 because FIA_UAU.2 is hierarchical to FIA_UAU.1.
FTP_TRP.1	FDP_UCT.1, under this profile, does not consider FDP_TRP.1 within the scope of profile.
Assurance Requirements	
ADV_HLD.1	ATE_DPT.1, AVA_SOF.1, AVA_VLA.1 no longer requires the ADV_HLD.1 dependency because the application will provide security enforcing high-level design (ADV_HLD.2) instead of descriptive high level design in order to meet EAL 3.

6.4 Security Functional Requirements Grounding in Objectives

Table 6-6 Requirements to Objectives Mapping

Requirements	Objectives
ACM_CAP.3	O.Apply_Code_Fixes, O.Crypto_Operation, O.Data_Exchange_Conf
ACM_SCP.1	O.Apply_Code_Fixes, O.Crypto_Operation, O.Admin_Guidance
ADO_DEL.1	O.Apply_Code_Fixes. O.Admin_Guidance
ADO_IGS.1	O.Apply_Code_Fixes. O.Admin_Guidance
ADV_FSP.1	O.Crypto_Key_Man, O.Crypto_Operation
ADV_HLD.2	O.Apply_Code_Fixes. O.Admin_Guidance, O.Crypto_Test_Reqs, O.Crypto_Operation, O.Atomic_Functions
ADV_RCR.1	O.Crypto_Key_Man, O.Crypto_Operation
ADV_SPM.1	O.Crypto_Key_Man, O.Crypto_Operation
AGD_ADM.1	O.Admin_Guidance, O.Apply_Code_Fixes, O.I&A, O.NonRepud_Assess_Recd, O.NonRepud_Assess_Sent, O.NonRepudiate_Sent, O.User_Auth_Management, O.NonRepudiate_Recd
AGD_USR.1	O.I&A, O.NonRepud_Assess_Recd, O.NonRepud_Assess_Sent, O.NonRepudiate_Sent, O.User_Auth_Management, O.NonRepudiate_Recd
ALC_DVS.1	O.Apply_Code_Fixes, O.Crypto_Operation, O.Admin_Guidance
ATE_COV.2	O.Crypto_Test_Reqs
ATE_DPT.1	O.Crypto_Test_Reqs

Requirements	Objectives
ATE_FUN.1	O.Crypto_Test_Reqs
ATE_IND.2	O.Crypto_Test_Reqs
AVA_MSU.1	O.Admin_Guidance
AVA_SOF.1	O.Crypto_Test_Reqs
AVA_VLA.1	O.Crypto_Key_Man, O.Crypto_Test_Reqs
FAU_GEN.1	O.Adm_User_Att_Mod, O.Audit
FAU_GEN.2	O.Adm_User_Att_Mod, O.Audit
FAU_SAR.3	O.Audit
FAU_SEL.1	O.Audit
FAU_STG.1	O.Audit
FAU_STG.4	O.Audit
FCO_NRO.1	O.NonRepud_Assess_Sent, O.NonRepudiate_Sent
FCO_NRR.1	O.NonRepud_Assess_Recd, O.NonRepudiate_Recd
FCS_COP.1	O.Data_Exchange_Conf.
FDP_ACC.2	O.AC_Admin_Limit, O.Crypto_AC, O.Crypto_Key_Man, O.Data_Exchange_Conf, O.Obj_Attr_Integrity, O.User_Attributes, O.User_Auth_Management
FDP_ACF.1	O.AC_Admin_Limit, O.Crypto_AC, O.Crypto_Key_Man, O.Obj_Attr_Integrity, O.User_Attributes, O.User_Auth_Management
FDP_IFC.1	O.Labels
FDP_IFF.1	O.Labels
FDP_ITC.1	O.Data_Exchange_Conf.
FDP_ROL.1	O.Clean_Obj_Recovery, O.Rollback
FDP_UCT.1	O. Data_Exchange_Conf

Requirements	Objectives
FDP_UIT.1	O.Active_Content, O.MsgMod_ID, O.General_Integ_Checks, O.Storage_Integrity
FIA_UAU.2	O.Adm_Limits_Bindings, O.Adm_User_Att_Mod, O.I&A, O.Limit_Actions_Auth
FIA_UAU.5	O.I&A
FIA_UAU.7	O.I&A
FIA_UID.1	O.I&A
FIA_USB.1	O.Adm_Limits_Bindings, O.I&A
FMT_MOF.1	O.Audit, O.Apply_Code_Fixes, O.Clean_Obj_Recovery, O.I&A, O.NonRepud_Assess_Recd, O.NonRepud_Assess_Sent, O.NonRepudiate_Sent, O.Security_Func_Mgt, O.NonRepudiate_Recd
FMT_MSA.1	O.Adm_User_Att_Mod, O.Apply_Code_Fixes, O.Crypto_Key_Man, O.Obj_Attr_Integrity, O.Security_Attr_Mgt, O.User_Auth_Management
FMT_MSA.2	O.Obj_Attr_Integrity, O.Security_Attr_Mgt, O.User_Attributes, O.User_Auth_Management
FMT_MSA.3	O.Data_Imp_Exp_Control, O.Obj_Attr_Integrity, O.Security_Attr_Mgt, O.User_Attributes, O.User_Auth_Management
FMT_MTD.1	O.Adm_Limits_Bindings, O.Crypto_Key_Man, O.Storage_Integrity
FMT_REV.1	O.User_Auth_Management, O.User_Attributes, O.User_Auth_Management
FMT_SMR.1	O.Audit, O.Obj_Attr_Integrity,

Requirements	Objectives
	O.Security_Roles, O.User_Attributes, O.User_Auth_Management
FPT_AMT.1	O.Crypto_Test_Reqs
FPT_RCV.3	O.Atomic_Functions
FTA_MCS.1	O.Limit_Mult_Sessions
FTA_SSL.3	O.Session_Termination

Appendix A - Acronyms

CC - Common Criteria
EAL - Evaluation Assurance Level
IT - Information Technology
PP - Protection Profile
SF - Security Function
SFP - Security Function Policy

S/MIME – Secure Multi-purpose Internet Mail Extension

SMPP – Secure Messaging Protection Profile
SMTP - Simple Mail Transfer Protocol

SOF - Strength of Function
ST - Security Target
TOE - Target of Evaluation
TSC - TSF Scope of Control
TSF - TOE Security Functions
TSFI - TSF Interface
TSP - TOE Security Policy